

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-174796
(43)Date of publication of application : 23.08.2000

(51)Int.CI.

H04L 12/46
H04L 12/28
H04L 9/32
H04L 12/66
H04L 12/56
H04L 29/14

(21)Application number : 10-347235

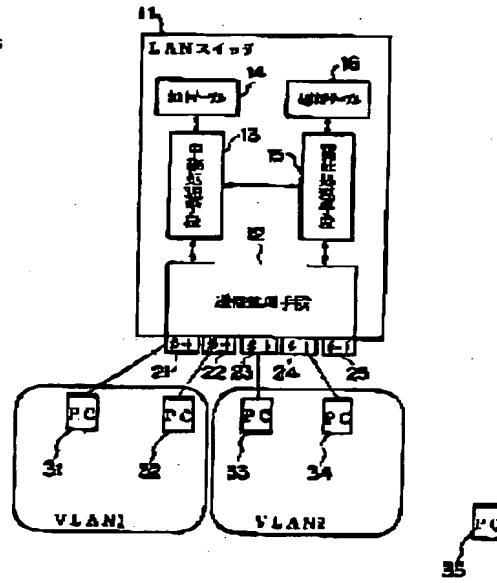
(71)Applicant : HITACHI LTD
(72)Inventor : TSUCHIYA KAZUAKI
NOZAKI SHINJI

(54) MANAGEMENT METHOD FOR COMMUNICATION NETWORK SYSTEM, AND INFORMATION REPEATER

(57)Abstract:

PROBLEM TO BE SOLVED: To facilitate the prevention of eavesdropping and impersonation by a malicious user and the analysis and restoration of an address setting error.

SOLUTION: An LAN switch 11 constitutes the communication network of a virtual LAN(VLAN) 1 and the VLAN 2, etc., by arbitrarily connecting plural personal computers(PCs) 31-34 as network terminals to respective plural ports 21-25. In this case, it is provided with a communication processing means 12 for transmitting and receiving packets with the respective ports 21-25, a relay processing means 13 for relaying the packets with the respective ports 21-25 based on a host table 14 updated by learning the change of the correspondence relation of the respective ports and the address information of the connected PC and an authentication processing means 15 for performing user authentication to the PC of a transmission origin by referring to an authentication table 16 and permitting the rewrite of the host table 14 and the relay of the packet only in the case of a true user at the time of the updating of the host table 14 of a packet relay trigger.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-174796

(P2000-174796A)

(43)公開日 平成12年6月23日 (2000.6.23)

(51)Int.Cl.	識別記号	FI	データー(参考)
H 04 L 12/46		H 04 L 11/00	3 10 C 5 J 10 4
12/28		9/00	6 75 A 5 K 03 0
9/32		11/20	B 5 K 03 3
12/66			1 0 2 D 5 K 03 5
12/56		13/00	3 11 9 A 00 1

審査請求 未請求 障求項の数 3 OL (全 14 頁) 最終頁に続く

BEST AVAILABLE COPY

(21)出願番号 特願平10-347235

(22)出願日 平成10年12月7日 (1998.12.7)

(71)出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(72)発明者 土屋 一晴
神奈川県海老名市下今泉810番地 株式会
社日立製作所サーバ開発本部内
(72)発明者 野崎 信司
神奈川県海老名市下今泉810番地 株式会
社日立製作所サーバ開発本部内
(74)代理人 100080001
弁理士 齋井 大和

最終頁に続く

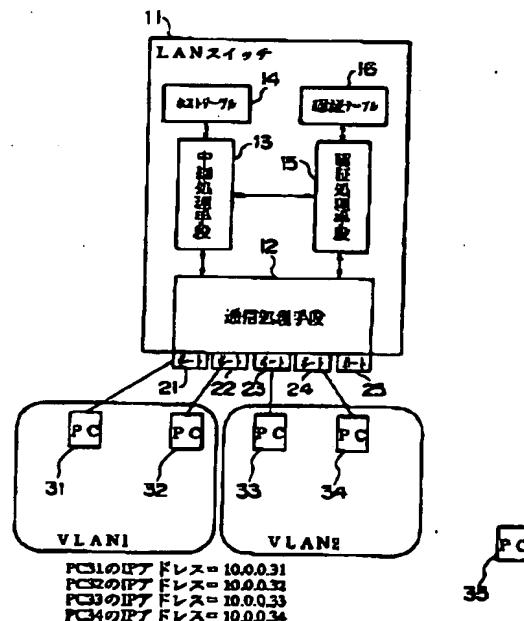
(54)【発明の名称】通信ネットワークシステムの管理方法および情報中継装置

(57)【要約】

【課題】 惡意のユーザによる盗聴やなりすましの防
止、アドレス記定ミスの解析や回復を容易にする。

【解決手段】 様数のポート21～25の各々に任意に
ネットワーク端末としての複数のPC31～34を接続
することでVLAN1およびVLAN2等の通信ネット
ワークを構成するLANスイッチ11において、各ポート
21～25との間でパケットの送受信を行う通信処理
手段12と、各ポートと、接続されたPCのアドレス情
報との対応関係の変化を学習して更新されるホストテー
ブル14に基づき各ポート21～25間のパケットの中
継を行う中継処理手段13と、パケット中継契機のホス
トテーブル14の更新時に、認証テーブル16を参照し
て送信元のPCに対してユーザ認証を行い、真正のユー
ザの場合にのみホストテーブル14の書き換えおよびパ
ケットの中継を許可する認証処理手段15とを備えた。

図 1



【特許請求の範囲】

【請求項1】 ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末またはネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置を用いた通信ネットワークシステムの管理方法であって、個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードとが対応付けて格納された認証テーブルを設定する第1のステップと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方のユーザに対して、前記ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およびパスワードと照合するユーザ認証を実行し、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する第2のステップと、
を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項2】 請求項1記載の通信ネットワークシステムの管理方法において、

前記第1のステップでは、前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方に対して、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスも対応付けて設定し、前記第2のステップでは、前記ユーザ認証にて前記通信情報の送信元または送信先の前記ユーザから入力された前記ユーザ名を含むとともに前記制御テーブルの更新要求が発生したことを通知するメッセージを作成して該当する前記ネットワーク論理アドレスまたはネットワーク物理アドレスの前記ユーザおよび管理者の少なくとも一方の連絡先メールアドレスに対して送出する処理、

前記第2のステップでの前記ユーザ認証に失敗したと

き、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに当該通信情報を受信した前記入出力ポートの切り離し、および当該入出力ポートから受信した全ての通信情報を廃棄する処理、

前記第2のステップでの前記ユーザ認証に失敗したとき、前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄し、さらに該通信情報の送信元の前記ネットワーク論理アドレスまたはネットワーク物理アドレスと同一の仮想LAN（ローカル・エリア・ネットワーク）に属す全ての前記ネットワーク端末のユーザに、前記ネットワーク論理アドレスまたはネットワーク物理アドレス等の設定ミスや、悪意のユーザが他のネットワーク端末のアドレスを使って盗聴やなりすましの通信を行おうとしている可能性があることを警告するメッセージを作成して送る処理、

前記制御テーブルの更新要求発生の有無に関係なく、定期的または不定期に前記制御テーブル内に登録された前記ネットワーク論理アドレスまたはネットワーク物理アドレスのユーザに対して前記ユーザ認証を実行する処理、

の少なくとも一つの処理を実行することを特徴とする通信ネットワークシステムの管理方法。

【請求項3】 ネットワーク端末またはネットワーク中継装置が接続される複数の入出力ポートと、個々の前記入出力ポートと前記ネットワーク端末またはネットワーク中継装置に付与されたネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方を対応付けて格納する制御テーブルと、前記制御テーブルに基づいて複数の前記入出力ポートの各々に接続された前記ネットワーク端末またはネットワーク中継装置の相互間での通信情報の授受を行うとともに、前記通信情報に含まれる前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と前記入出力ポートとの対応関係の変化を学習して前記制御テーブルを更新することで、前記入出力ポートに対する前記ネットワーク端末またはネットワーク中継装置の接続状態の動的な変更を可能にする中継処理手段とを含む情報中継装置であって、

個々のネットワーク端末に対応した前記ネットワーク論理アドレスおよびネットワーク物理アドレスの少なくとも一方と、当該ネットワーク端末のユーザ名およびパスワードと、前記ユーザおよび通信ネットワークシステムの管理者の少なくとも一方の連絡先メールアドレスが対応付けて格納された認証テーブルと、

前記制御テーブルの更新を伴う前記通信情報の授受が発生した時、前記通信情報の授受および前記制御テーブルの更新に先立って、前記通信情報の送信元および送信先の少なくとも一方の前記ユーザに対して、ユーザ名およびパスワードの入力を要求し、入力されたユーザ名およびパスワードと前記認証テーブル内の前記ユーザ名およ

びパスワードと照合するユーザ認証を実行するとともに、前記通信情報の送信元および前記管理者の少なくとも一方の前記送信先メールアドレスに対して前記ユーザ認証で得られた前記ユーザ名と前記制御テーブルの更新要求が発生したことを通知するメッセージを送信するとともに、前記ユーザ認証に成功したときのみ前記制御テーブルの更新および前記通信情報の授受を実行し、前記ユーザ認証に失敗したときは前記制御テーブルの更新を抑止するとともに前記通信情報を廃棄する動作を行う制御論理と、

を備えたことを特徴とする情報中継装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、通信ネットワークシステムの管理技術および情報中継技術に関し、特に、LAN (LAN: Local Area Network) スイッチ (Layer2スイッチ、Layer3スイッチ等) と呼ばれるインターネットワーク装置、およびLANスイッチで構成する通信ネットワークシステム (LANスイッチネットワークシステム) の管理方法等に適用して有効な技術に関する。

【0002】

【従来の技術】LANスイッチが有する特徴技術にVLAN (VLAN: Virtual LAN) がある。VLANはインターネット装置の物理的なポートに依存せずにLANの構築を可能にする技術であり、その形式の違いによってポートベースVLAN、MAC (MAC: Media Access Control) アдресベースVLAN、Layer3プロトコルベースVLAN、IP (IP: Internet Protocol) サブネットベースVLAN等の名称で知られている。

【0003】本発明の参考技術では、例えば図7に示すIPサブネットベースVLANの通信ネットワークシステムにおいて複数のポート221～225を備えたLANスイッチ200はPC (PC: Personal Computer) 231からPC233へのパケットを受信すると、パケットの始点MACアドレス、終点MACアドレス、始点IPアドレスを学習してホストテーブル220を作成する。次に終点IPアドレスをキーにホストテーブル220を参照し、該当エントリが有る場合は、該当ポートにパケットを出力する。該当エントリが無い場合は、ルーティングテーブル (図示無し) およびARP (ARP: Address Resolution Protocol) テーブル (図示無し) を参照してネクストホップを決め、該当するホストテーブル220のエントリを新規に作成して、該当ポートにパケットを出力する。LANスイッチ210はこのようにしてPC231からPC233へのパケットを中継する。

【0004】さらにLANスイッチ210では、定期的にホストテーブル220のエントリを廃棄し、新たにパケットから学習することによって常にホストテーブル220のエントリを更新しているため、PCが移動した場合でも移動先のポートにパケットを正しく中継すること

ができる。すなわちPCは移動した場合でも移動前と同様の通信を自動的に再開することができる。

【0005】

【発明が解決しようとする課題】しかしながら、上記参考技術には、次の技術的課題がある。

【0006】第1の技術的課題は、IPアドレス等の設定ミスに対して無防備なことである。例えばPC232がPC231のIPアドレスを誤って設定、ポート222に接続してしまったとする。この場合、LANスイッチ210ではPC231がポート221からポート222に移動したと判断し、そのようにホストテーブル220を書き換えてしまう。この結果、IPアドレスを正しく使用しているPC231が通信出来なくなる等の通信不良が発生する。また、ネットワークに接続されるPCの数が多い場合には、この通信不良の解析や回復には、多大の労力を要する。

【0007】第2の技術的課題は、悪意のユーザによる盗聴やなりすましを許してしまうことである。例えばPC235がPC231のIPアドレスを設定、ポート225に接続したとする。この場合、LANスイッチ210ではPC231がポート221からポート225に移動したと判断し、そのようにホストテーブル220を書き換えてしまう。この結果、PC235がPC231宛の通信データを受け取って盗聴したり、またPC231になりすまして通信できてしまう。

【0008】本発明の目的は、論理的あるいは物理的なネットワークアドレス等の設定ミスによる通信不良の防止や通信不良の原因解析および回復操作の迅速化が可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

【0009】本発明の他の目的は、悪意のユーザによる盗聴やなりすましを防ぐことで通信ネットワークシステムのセキュリティを向上させることができ可能な通信ネットワークシステムの管理技術および情報中継技術を提供することにある。

【0010】

【課題を解決するための手段】本発明は、LANスイッチ等の情報中継装置に備えられた複数の入出力ポートにユーザ端末や他の中継装置を接続して構築され、入出力ポートに対するユーザ端末等の接続状態の変化を学習して、入出力ポートとネットワークアドレスとの対応関係を管理する制御テーブルを更新することで、個々のユーザ端末の入出力ポートに対する接続状態を動的に変更することが可能な通信ネットワークの管理方法において、各ユーザ端末間、すなわち複数の入出力ポート間で通信情報の授受を契機とする制御テーブルの更新要求が発生した時、当該通信情報の送信元のユーザ端末に対してユーザ認証を実行し、真正のユーザであることが確認された場合にのみ、制御テーブルの更新およびそれに基づく通信情報の授受を行わせるものである。